

M&G No. 2968.215USU1

**REMOTE PERSONALIZATION AND ISSUANCE OF
IDENTITY DOCUMENTS**

This application claims priority from provisional application Serial No.
5 60/412,267, filed September 20, 2002, and which is incorporated herein by reference.

Field of the Invention

This invention relates to the production and issuance of identity documents. In particular, this invention relates to table top units that are able to personalize and issue secure identity documents, including cards such as national ID
10 cards, drivers licenses and the like, and booklets such as passports and the like.

Background of the Invention

Personalization and issuance of identity documents, such as national ID cards, drivers licenses, passports and the like must be done in a highly secure manner in
15 order to ensure the integrity and distribution of the issued identity documents. The security concerns surrounding the issuance of these types of identity documents includes the prevention of document forgeries and duplications, issuance of a document to a person other than for whom the document was created, and issuance to unauthorized persons such as criminals.

20 To ensure the integrity of identity documents, such documents have typically been personalized and issued by a central issuing agency or location, such as a local or federal governmental authority. These documents are often sent to the intended recipient through the mail. However, mail systems throughout the world often times cannot be sufficiently relied upon. In addition, documents can be stolen from the mail
25 prior to reaching the intended recipients.

As an alternative to mail, the issuing agency may require the intended document recipient to appear personally at the issuing agency to personally retrieve the issued document. This can often times be inconvenient for the recipient who may be located far away from the site of the issuing agency. There are also instances when a

person needs a replacement identity document such as when the previous identity document is lost, stolen and/or damaged. It can also be inconvenient for a person to go to the issuing agency to obtain a replacement.

De-centralized personalization and issuance of identity documents would
5 resolve these problems and others. However, de-centralized personalization and issuance must be done in a manner to ensure the integrity and distribution of the issued identity document.

A previous attempt at de-centralized issuance of personalized financial cards is disclosed in WO 92/17856. As described therein, financial cards that contain
10 user specific information are issued at a remote, unattended location directly to the user at an ATM-like machine.

There is, however, a continuing need for de-centralized personalization and issuance of identity documents.

Summary of the Invention

15 The invention provides a system for personalizing and issuing identity documents such as national ID cards, drivers licenses and the like, and booklets such as passports and the like, at a location remote from a central issuing agency. The system permits remote personalization and issuance of documents under mobile conditions while ensuring the security and integrity of the issuance process. The system operates
20 under local control by an operator, but requires authorization from a remote authority prior to any personalization procedures or document issuance.

The invention also provides table top personalization machines that are used in the system for personalizing documents. Each table top machine is designed to be readily portable to facilitate mobile operations. Preferably, a machine includes a
25 single personalization unit to promote the mobility of the machines. The machines interface with a local PC under operator control, and each includes the capability of interfacing with a remote central agency from which authorization must be received prior to personalizing or issuing any document.

A series of procedures to help ensure the security of the personalization and issuance process are also provided. These procedures provide the remote agency with full control of the personalization and issuance process. The procedures include remote enabling of machine operation, operator authorization for every machine step, authorization of the data sought to be personalized onto the document, logging of the machine operations, and logging of the documents emitted from the machine.

For a better understanding of the invention, its advantages and objects obtained by its use, reference should be made to the drawings which form a further part hereof, and to the accompanying description, in which there is described a preferred embodiment of the invention.

Brief Description of the Drawings

Figure 1 illustrates the de-centralized document personalization and issuance system of the invention.

Figure 2 is a block diagram of the remote enabling feature of the invention.

Figure 3 is a block diagram of the operator authorization feature of the invention.

Figure 4 is a block diagram of the data set authorization feature of the invention.

Figure 5 is a block diagram of the machine operations logging feature of the invention.

Figure 6 is a block diagram of the document logging feature of the invention.

Detailed Description

Figure 1 illustrates a de-centralized document personalization and issuance system 10 according to the present invention. The system 10 includes a portable, table top personalization machine 12 which personalizes an identity document 14. Identity documents which can be personalized using the system of the invention

includes cards such as national ID cards, drivers licenses and the like, and booklets such as passports and the like. Therefore, the terms "identity document" and "document" used herein are intended to include both cards and booklets.

5 The identity document 14 can be a document without any previous personalization, or a document with previous personalization whereby the machine 12 adds additional personalization to the document. Documents to be personalized are preferably input into the machine 12 one-by-one, and after personalization, are emitted from the machine. The documents can be fed into the machine by hand or by a suitable mechanized process which feeds the documents from a supply of documents, e.g. using
10 an input hopper.

The table top machine 12 includes a personalization unit 16 which personalizes the document 14, a control unit 18 which controls operation of the machine 12, a Global Positioning System (GPS) receiver 20, and a Global System for Mobil Communications (GSM) transceiver 22. The type of personalization unit 16 that is used
15 will depend upon the intended use of the table top machine. Preferably, a single personalization unit 16 is provided to promote the portability of the machine 12. However, it is contemplated that more than one personalization unit could be provided.

In one embodiment, the table top machine 12 is for personalizing plastic identification cards. In this case, the personalization unit 16 that is preferably used is a
20 laser engraving unit that performs laser engraving on the plastic card 14. Laser engravers produce high resolution text and images on documents, which make the documents difficult to alter or forge. Photos, text, bar codes, fingerprints, microprinting, signatures and other graphic elements can be added to the identification card by the laser engraving unit. Laser engraving units for personalizing documents are
25 well known in the art. In this type of machine 12, the plastic cards 14 to be personalized are preferably provided from an input hopper mechanism forming part of, or connected to, the table top machine 12. If desired, the machine 12 can also include an output stacker that stacks personalized cards.

In another embodiment, the table top machine 12 is for personalizing
30 passports. In this case, the personalization unit 16 that is used is preferably a laser

engraving unit that performs laser engraving on the passport 14. In this type of machine, a passport to be personalized is fed by hand into the machine 12. Photos, text, bar codes, fingerprints, microprinting, signatures and other graphic elements can be added to the passport by the laser engraving unit. A system for personalizing passports
5 is disclosed in copending Application Serial No. 09/768,449, filed on January 24, 2001, entitled "Passport Production System and Method".

In yet another embodiment, the personalization unit 16 in the machine 12 is preferably an ink-jet printer for personalizing documents that are compatible with ink-jet printing.

10 The machine 12 could also be provided with integrated circuit (IC) chip programming capability, either in place of the personalization units 16 mentioned above, or in addition to the above-described personalization units 16, in which case the machine 12 will include a plurality of personalization units. Many documents are now being provided with IC chips embedded therein to increase the amount of data that can
15 be stored on the document. The IC chip programming unit which would perform programming operations on the IC chip can either be of the contact or contactless type, each of which is known in the art. The machine 12 can include other personalization capabilities as well, in addition to those described above.

In the preferred embodiment, the machine 12 is designed to permit
20 personalization operations away from a central location under mobile conditions. Therefore, in the preferred embodiment, the machine 12 includes a single personalization unit 16 to promote the mobility of the machine. However, it is contemplated that the machine 12 could include additional personalization units as well while still permitting mobile operations.

25 The control unit 18 of the machine 12 controls operation of the personalization unit 16. The techniques for controlling a personalization unit to perform a desired personalization function are known in the art. In addition, the control unit 18 is connected to the GPS receiver 20 whereby the control unit 18 knows the exact location of the machine 12 at all times. The control unit 18 further communicates with
30 a remote central agency 24 via the GSM transceiver 22, and with a local controller, such

as a local PC 26, through a suitable interface, such as an ethernet connection 28. The central agency 24 can be a governmental authority that regulates the issuance of the documents 14, or some other authorized entity. Communications between the control unit 18 and the central agency 24 are encrypted using known encryption techniques, with an encryption unit 30 of the machine 12 encrypting communications sent from the control unit 18 to the central agency 24 and decrypting communications received from the central agency 24.

The system 10 operates as follows: a document 14 to be personalized is fed into the machine 12. The personalization unit 16 then performs a personalization process on the document under control of the control unit 18. For example, the personalization unit 16 can be a laser engraving unit that can laser engrave personal data or a picture of the document recipient onto the document. After personalization is complete, the document is discharged from the machine 12.

The GPS receiver 20 and GSM transceiver 22 permit mobile operations of the machine 12, thereby enabling de-centralized issuance of documents. Yet operation of the machine 12 must be such that the security and useability of the machine 12, and the resulting security of issued documents, is ensured. A series of procedures to help ensure the security of the operation of the machine 12 and the issuance of documents will now be described.

20

Remote Enabling of Machine Operation

As described above, the machine 12 permits mobile operations remote from the central agency 24. However, to increase security, the central agency is provided with full control to enable machine operations. Without enable authorization from the central agency, the machine 12 will not operate and personalization of documents is not possible, thereby preventing unauthorized usage of the machine 12.

Figure 2 illustrates the remote enabling process 40. At block 41, the power to the machine 12 is turned on, and thereafter the machine is initialized at block 42. The control unit 18 then obtains the current geographic location of the machine 12 from the GPS receiver 20 at block 43. Local operator authorization is then input at

block 44 by an operator of the PC 26 entering a personal identification number via a keyboard or other PC interface device which is sent to the control unit 18. In addition, biometric data unique to the operator, such as a fingerprint, can be used to further increase security. A fingerprint can be obtained using a fingerprint sensor on the machine 12 or provided as part of the PC 26, with the fingerprint data being sent to the control unit 18. Other biometric data unique to the operator could be utilized as well. For example, an iris scanner can be used to scan the operator's iris and send the data to the control unit 18.

At block 45, the control unit 18 then sends an enable request to the central agency 24 via the GSM transceiver 22. The enable request includes the current geographic location of the machine obtained from the GPS receiver, the ID number of the operator, and a serial number unique to the machine 12. The biometric data, if obtained, can also be sent to the central agency 24 as part of the enable request. The control unit 18 then waits for enable permission from the central agency 24. Until permission is received, no further action is possible.

At block 46, the central agency 24 checks the information in the enable request against centrally stored data. A discrepancy between the information in the enable request and the centrally stored data could indicate that the machine 12 is not in its expected location, the operator is not the expected operator, and/or the machine is not the expected machine. Any one of these discrepancies may indicate a security breach or unauthorized use of the machine. If a discrepancy exists, the central agency does not send operation permission back to the machine 12 and the machine cannot operate. Provided that no discrepancy exists, the central agency 24 sends back an enable permission signal to the control unit 18 at block 47. The control unit 18 then prepares for a personalization operation at block 48.

Operator Authorization

The table top machine 12 works under local operator control during usual operation. Even after machine operations are enabled, there is a continuing need to control machine operation to prevent security lapses from occurring once enable

permission is given. The system 10 is designed such that every single machine step that requires operator intervention needs authorization from the local operator and from the central agency, thereby preventing unauthorized personnel access to the machine. Absent these authorizations, no single machine action is possible.

5 Figure 3 illustrates the operator authorization process 50. At block 51, the operator selects the intended action using the PC 26, and at block 52, the operator inputs a personal identification number and, if utilized, biometric data. The control unit 18 then sends an authorization request to the central agency 24 at block 53, which checks the information in the authorization request against centrally stored data at block
10 54. Provided no discrepancies in the information exist, the central agency 24 sends back authorization for the intended action at block 55. If a discrepancy exists, the selected action is not authorized and the machine is prevented from performing the action. Once authorization is received, the control unit 18 starts the selected action at block 56. This process is repeated for each action that is requested of the machine by
15 the operator.

Data Set Authorization

The table top machine 12 not only works under local operator control, but it also performs personalization based upon locally collected data, such as data input
20 via the PC 26. To provide the central agency 24 with full control of the data that is being entered onto the documents and control of persons receiving personalized documents, every data set sought to be entered onto a document must first be authorized by the central agency. This facilitates detection of criminals and unauthorized persons attempting to receive documents.

25 Figure 4 illustrates the data set authorization process 60. At block 61, a data set that is to be personalized onto the document is entered by the operator of the PC 26. This data set is sent to the control unit at block 62, which then sends, at block 63, an authorization request to the central agency. The authorization request includes the data set, machine location information, operator ID and machine serial number, as well
30 as biometric data if utilized. At block 64, the authorization request is checked against

centrally stored data, and thereafter, assuming that no discrepancies exist, the central agency 24 sends back an authorization to the control unit 18 at block 65. If a discrepancy exists, the machine is prevented from personalizing the document with the selected data set. Once authorization is received, the control unit starts the
5 personalization of the document with the data set at block 66.

Machine Operations Logging

As further added security, the system 10 also provides the central agency 24 with full control of mobile operations by logging all machine operations with the
10 central agency.

Figure 5 illustrates the machine operations logging procedure 70. At block 71, the control unit 18 initiates a personalization action of the personalization unit 16. The control unit 18 then sends a log report to the central agency at block 72. The control unit then waits for completion of the personalization action, block 73, and a
15 report from the personalization unit 16, block 74, that the action is complete and the result of the action. The control unit 18 then sends another log report including the action result to the central agency 24 at block 75.

If the central agency 24 spots any impropriety in the log reports and action results, it can suspend operation of the machine 12 to allow investigation into the
20 impropriety.

Document Logging

The system 10 also provides the central agency 24 with full control of the personalized documents, whereby every personalized document is logged with the
25 central agency for tracking purposes.

Figure 6 illustrates the document logging process 80. At block 81, the control unit 18 checks for completion of the document personalization process. After the machine completes a personalization action on a document, the document is emitted from the machine to the operator or the intended user of the document. The control unit
30 then sends a document emitted report to the central agency at block 82, which collects

the report. In this manner, the central agency knows that a document has been produced for a user.

The system environment for all machines 12 described herein is generally the same, including at least one personalization unit 16, a control unit 18, GPS
5 capability, GSM capability, encryption capability, and optionally operator biometrics capability.

The above specification, examples and data provide a complete description of the invention. Many embodiments of the invention, not explicitly described herein, can be made without departing from the spirit and scope of the
10 invention.